REMARKS

This communication is a full and timely response to the final Office Action dated September 28, 2005 (Paper No./Mail Date 90202005). By this communication claims 1, 4, 6, 10, 12, and 17 have been amended.

Claim 1 has been amended to recite that said public key certificate includes at least a basic area and an extended area. Support for the subject matter recited in claim 1 can be found variously throughout the claims and specification, for example, in original claim 4 and in paragraphs [0138] and [0139] of corresponding U.S. Patent Application Publication No. 2002-0108041. No new matter has been added.

Claim 6 has been amended to recite storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; and generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data. Support for the subject matter recited in claim 6 can be found variously throughout the claims and specification, for example, in original claim 10 and in paragraphs [0138] and [0139] of corresponding U.S. Patent Application Publication No. 2002-0108041. No new matter has been added.

Claim 17 has been amended to recite storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a first signature based on the a first signature algorithm derived from the stored basic data and extended data; and attaching the first digital signature to the public key certificate. Support for the subject matter recited in claim 17 can be found variously throughout the specification, for example, in paragraphs [0138] and [0139] of corresponding U.S. Patent Application Publication No. 2002-0108041. No new matter has been added.

Claims 4 and 10 have been amended to address formal matters. No new matter has been added.

Entry of this Amendment is proper under 37 C.F.R. §1.116 since the amendment: (a) places the application in condition for allowance (for the reasons discussed herein); (b) satisfies a requirement of form asserted in the previous Office Action; and (c) places the application in better form for appeal, should an appeal be necessary. The amendment is necessary and was not earlier presented because it is made in response to arguments raised in the final rejection. Entry of this amendment is respectfully requested. Reexamination and reconsideration in light of the above amendments and the following remarks is respectfully requested.

Claims 1-12 and 17 are pending where claims 1, 6, 12, and 17 are independent.

Rejections Under 35 U.S.C. §103

Claims 1, 2, 6, 8, and 12-17 were rejected under 35 U.S.C. §103(a) as unpatentable over *Shear et al.*--U.S. Patent No. 6,157,721 in view of *Whittle*—"Public Key Authentication Framework: Tutorial," First Principles Consulting, 2 June 1996. Applicant respectfully traverses this rejection.

Claim 1 recites a public key certificate issuing system comprising a certificate authority for issuing a public key certificate of an entity which uses said public key certificate; and a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority; said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority, attaching a digital signature on message data constituting said public key certificate in accordance with said different signature algorithm at each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms, wherein said public key certificate includes at least a basic area and an extended area.

Claim 6 recites a public key certificate issuing method having a certificate authority for issuing a public key certificate of an entity which uses said public key certificate and a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority to issue said public key certificate in response to said public key certificate issuing request from said registration authority, said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, including the steps of storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data; transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority; attaching the digital signature on message data constituting said public key certificate in accordance with said different signature algorithm at each certificate authority; and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms.

Claim 12 recites information processing apparatus for executing verification of a public key certificate, having a configuration for selecting, from among a plurality of signature algorithms recorded in signature information stored in a basic area and an extended area of said public key certificate, a signature algorithm which can be verified by said information processing apparatus and executing signature verification on the basis of the selected signature algorithm.

Claim 17 recites a program storage medium for providing a computer program for executing public key certificate issuing processing for issuing a public key certificate of an entity which uses said public key certificate, said computer program comprising the steps of storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a first signature based on the a first signature algorithm derived from the stored basic data and extended data; attaching the first digital signature to the public key certificate; generating, with the use of a second signature algorithm different from that of the first signature attached to said public key certificate, a second signature and attaching said second signature to said public key certificate.

In summary, claims 1 and 12 similarly recite that the public key certificate includes a basic area and an extended area. In addition, claims 6 and 17 recite storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data.

Shear discloses that one digital signature 106(1) can be created by encrypting message digest 116 with a private key 122(1), another (different) digital signature 106(2) can be created by encrypting the message digest 116 with a different private key 122(2), possibly employing a different signature algorithm, and a still different digital signature 106(N) can be generated by encrypting the message digest using a still different private key 122(N), possibly employing a different signature algorithm. *See* col. 14, line 63 through col. 15, line 6. The Office Action acknowledges that *Shear* fails to disclose, teach, or suggest at least a registration authority, as recited in the claims. In addition, Applicant submits that *Shear* also fails to disclose, teach, or suggest at least that the public key certificate includes a basic area and an extended area, as recited in claims 1 and 12, and recite storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data, as recited in claims 6 and 17.

Whittle discloses a Public Key Authentication Framework that uses a registration authority for legitimizing and/or legalizing transactions performed through digital signatures. *Whittle*, however, fails to disclose, teach, or suggest at least the aforementioned elements of claims 1, 6, 12, and 17. Thus, *Whittle* fails to remedy the deficiencies of *Shear*, and as a result a *prima facie* case for obviousness has not been established.

In summary, *Shear* and *Whittle* either singly or combined fail to disclose, teach, or suggest at least that the public key certificate includes a basic area and an extended area, as recited in claims 1 and 12, and recite storing basic data in a basic area of the public key certificate; storing extended data in an extended area of the public key certificate; generating a digital signature based on a first signature algorithm derived from the stored basic data and extended data, as recited in claims 6 and 17. At best, the combined references teach that different encryption keys can be generated using the same algorithm of a single apparatus.

In relation to claim 10, the Office Action alleges that *Levi* (see infra) teaches storing a generated signature in an area other than a basic area and an extended area. However, the Office Action failed to establish at least that *Shear* and *Whittle* disclose that the private key certificate includes a basic area and an extended area. Thus, *Levi* also fails to remedy the deficiencies of both *Shear* and *Whittle*.

To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, obviousness "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys. V. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). For at least the above reasons, Applicant respectfully requests that the rejection of claim 4 be withdrawn, and claims 1, 6, and 17 be allowed.

Claim 2 depends from claim 1, and claim 8 depends from claim 6. By virtue of this dependency, Applicant submits that claims 2 and 8 are allowable for at least the same reasons given above concerning their respective base claims. In addition, Applicant submits that claims 2 and 8 are further distinguished over *Shear* and *Whittle* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 2 and 8 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claims 3 and 9 were rejected under 35 U.S.C. §103(a) as unpatentable over *Shear* and *Whittle*, and further in view of *Chokhani*—"Comment on RFC 2527, " The Internet Society, March 1999. Applicant respectfully traverses this rejection.

Claim.3 depends from claim 1 and claim 9 depends from claim 6. By virtue of this dependency, Applicant submits that claims 3 and 9 are allowable for at least the same reasons given above concerning their respective base claims. In addition, Applicant submits that claims 3 and 9 are further distinguished over *Shear, Whittle,* and *Chokhani* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 3 and 9 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claims 4 and 10 were rejected under 35 U.S.C. §103(a) as unpatentable over *Shear*, *Whittle*, and *Chokhani* and further in view of *Levi et al.*,--"A Multiple Signature Based Certificate Verification Scheme," Proceedings of BAS '98, The Third Symposium on Computer Networks, June 1998. Applicant respectfully traverses this rejection.

Claim 4 depends from claim 1 and claim 10 depends from claim 6. By virtue of this dependency, Applicant submits that claims 4 and 10 are allowable for at least the same reasons concerning their respective base claims. In addition, Applicant submits that claims 4 and 20 are further distinguished over *Shear, Whittle, Chokhani*, and *Levi* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 4 and 10 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claims 5 and 11 were rejected under 35 U.S.C. §103(a) as unpatentable over *Shear* and *Whittle* and further in view of *Levi*. Applicant respectfully traverses this rejection.

Claim 5 depends from claim 1 and claim 11 depends from claim 6. By virtue of this dependency, Applicant submits that claims 5 and 11 are allowable for at least the same reasons concerning their respective base claims. In addition, Applicant submits that claims 5 and 11 are further distinguished over *Shear, Whittle,* and *Levi* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 5 and 11 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Conclusion

Based on at least the foregoing amendments and remarks, Applicants submit that claims 1-12 and 17 are allowable, and this application is in condition for allowance. Accordingly, Applicants request favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicants request that the Examiner contact the undersigned attorney at the number listed below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2321 from which the undersigned is authorized to draw.

Dated: November 22, 2005

Respectfully submitted,

By________________
Ronald P. Kananen
Registration No.: 24,104
Shawn B. Cage
Registration No.: 51,522
Attorneys for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

DC210430